AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* THE PREMISES LOCATED AT: 1380 Hunters Hollow Ct. Eureka, Missouri 63025	Case No. 4:20 MJ 3199 NCC SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 2251(a) 18 U.S.C. Section 2252 18 U.S.C Section 2252A	Production, possession and/or receipt, and shipment of child pornography, and other related materials

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Applicant's signature

Gregory S. Marx, Special Agent, FBI

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: June 26, 2020

Judge's signature

City and state: St. Louis, MO

Noelle C. Collins, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT: 1380 Hunters Hollow Ct. Eureka, Missouri 63025	))))))))	No. 4:20 MJ 3199 NCC FILED UNDER SEAL SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Gregory S. Marx, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1380 HUNTERS HOLLOW CT., EUREKA, MISSOURI 63025 further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation's ("FBI") Violent Crimes Against Children Task Force. I have been an FBI agent for approximately 12 years. I have conducted numerous investigations regarding the sexual exploitation of children that involve the use of a computer which has been used to commit a crime in violation of Title 18, United States Code, Sections 2251(a), 2252 and 2252A. As an FBI Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors including computers, computer equipment, software, and electronically stored information. I have experience utilizing

computers during my career as an investigator and I have completed multiple in-service trainings and other courses in computer crime investigation.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2251(a), 2252 and 2252A have been committed by **STEVEN LEE GLOVER**, or other persons known and unknown. Sections 2251(a), 2252 and 2252A criminalize, among other things, the production, receipt, distribution, and possession of child pornography. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED

5. The premises to be searched is: 1380 HUNTERS HOLLOW CT., EUREKA, MO 63025, a single-family ranch home with an attached two-car garage. The Premises is further described in the photographs in Attachment A, and is referred to herein as the SUBJECT PREMISES.

DEFINITIONS

6. The following terms have the indicated meaning in this affidavit:

a. The term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly

related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. 18 USC § 1030(e).

b. The term "minor" means any individual under the age of 18 years. 18 USC § 2256(1).

c. Sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the anus, genitals, or pubic area of any person. 18 USC § 2256(2)(A).

d. Visual depiction includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).

e. Child pornography means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC § 2256(8)(A) or (C).

f. Identifiable minor means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual

person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 USC § 2256(9).

g. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including for example, tablets, digital music devices, portable electronic game systems, electronic game consoles and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

l. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

m. "Wireless telephone or mobile telephone, or cellular telephone" as used herein means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

PROBABLE CAUSE

7. On April 14, 2020, your Affiant was contacted regarding the solicitation via Instagram of nude photos from a minor female victim, S.E., by an individual utilizing the Instagram account "keegslaurent2019", screen name Keegan Laurent.

8. S.E.'s father discovered the images and Instagram chats while reviewing her phone. S.E.'s father initially assumed the user of keegslaurent2019 was 17 years of age, as purported. However, after reviewing the images and chats and speaking with his daughter, S.E.'s father, who formerly worked sex crime cases as a law enforcement officer, suspected the user of keegslaurent2019 could be an adult sex predator.

9. S.E.'s father identified a phone number provided to his daughter by the user of keegslaurent2019 as 636-428-5460.

10. S.E.'s father observed two images sent by his daughter to keegslarent2019, which he believed constituted child pornography. Said images were sent to keegslaurent2019 via Instagram messenger on April 7, 2020. S.E.'s father used S.E.'s phone to take screenshots of the images, in order to preserve them.

11. On April 15, 2020 a preservation request was sent to Facebook regarding Instagram account keegslaurent2019, for the period of April 15, 2018, to April 16, 2020. A preservation request was also provided to Facebook for S.E.'s Instagram account.

12. On April 21, 2020 a subpoena was served via the Facebook Law Enforcement Portal, for subscriber/recent login information regarding Instagram account keegslaurent2019.

13. Records received from Facebook on May 6, 2020 indicated the following subscriber/recent login IP information:

a. Name: Keegan Laurent

b. Email address: keegslaurent2019@gmail.com

c. Vanity Name: keegslaurent2019

d. Account Registration Date: 2019-07-13 19:45:09 UTC

e. Registration IP: 24.216.143.114

f. Multiple logins on various dates/times from IP 24.216.143.114

g. Most recent login IP: 24.216.143.114 Time 2020-03-22 11:44:25 UTC

14. On May 14, 2020 a subpoena was served to Charter Communications for subscriber information associated with IP address 24.216.143.114, at the dates and times specified in the records provided by Facebook for keegslaurent2019.

15. On May 19, 2020 records provided by Charter indicated the following subscriber information for IP address 24.216.143.114, for all the specified dates and times:

a. Subscriber name: Steven Glover

b. Subscriber address: 1380 Hunters Hollow Ct., Eureka, MO 63025

16. Department of Revenue and private source database queries fully identified Steven Lee Glover, date of birth XX/XX/1966, residential address 1380 Hunters Hollow Ct., Eureka, MO 63025.

17. On May 26, 2020 S.E.'s father provided your Affiant with the smartphone used by S.E. to communicate with keegslaurent2019. S.E.'s father signed a FD-26 Consent to Search form. The phone was identified as an Apple iPhone Xr, model A1984, serial # F2MZ26YTKXKN.

18. On June 6, 2020 your Affiant conducted a forensic extraction and analysis of data on captioned device. The following relevant information was noted:

a. Approximately 23 screenshot images of Instagram conversations between S.E. and keegslaurent2019 were extracted from the device.

b. A review of the screenshots indicated the conversations were sexual in nature. For example, keegslaurent2019 asks S.E. to "spread and show me from between your legs sexy", and "show me the nipples you want me to suck".

c. S.E. responded to keegslaurent2019 with images. Most of the image content was no longer visible in the messages.

d. However, three images were visible in one of the screenshots. The images are all similar in nature and are described as follows:

- A fully nude female, identified as S.E. by her father, is pictured from behind, in what appears to be her bedroom. Her face is not visible. The focal point of the image is her buttocks and vagina. She kneels on a bed with her left hand between her legs and her fingers in her vagina.

e. Keegslaurent2019 responded to the images described above with "Yes baby more like that and I'm going to cum in you" and "Try to spread your ass wide open for me."

19. On June 24, 2020 your Affiant conducted surveillance of 1380 Hunters Hollow Ct., Eureka, MO 63025. At approximately 5:18 p.m. a Hyundai with Missouri license plate KN2R7B pulled into the garage. A Missouri Department of Revenue query regarding said vehicle indicated it is currently registered to **Steven Glover.**

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

20. In my training and experience, I know that cellular phones ("smart phones"), contain software and hardware that are the same, if not more sophisticated, than a typical home computer. The term "computer," "hard drive," and "computer media," as used in this affidavit, also refers to cellular "smart" phones.

21. I also know that "smartphones" often allow for cloud-based storage, and many users back up their phones on their home computers. Information contained in a cell phone that is connected to a desktop, laptop computer, or the cloud, can easily transfer onto other media.

22. A computer's ability to store images in digital form makes a computer an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

23. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

24. Collectors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, iCloud, and Hotmail, and social media applications such as Kik and Snapchat among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer, even if the user is accessing the information on their cellular "smart phone." Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

25. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained

unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

26. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of

computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

27. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

28. In addition, there is probable cause to believe that the computer and its storage devices are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251(a), 2252, and 2252A, and should all be seized as such.

29. Affiant knows from training and experience that even if the files were deleted by a user, they still may be recoverable by a trained computer forensic examiner. Trained certified computer forensic examiners routinely extract incriminating deleted files from hard drives, usually without difficulty.

30. Since a deleted file is not overwritten all at once, it may be possible to reconstruct it from the bits of data composing it, called “slack data”.

31. It is difficult to know, prior to the search, which exact method of extracting the evidence will be needed and used and which specific expert possesses sufficient specialized skills to best obtain the evidence and subsequently analyze it. No matter which method is used, the data analysis protocols that will be utilized are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Upon approval and execution of the search warrant, in appropriate circumstances, a forensic image (also known as a bit-stream image), which is an exact physical copy of the seized electronic evidence, will be created so that their contents could be examined at a field office or computer laboratory and/or other locations following completion of the on-site search.

32. The search of computers, hard drives, and other seized electronic media will include a complete search of the entire piece of seized electronic evidence. A computer forensic examiner cannot rely on the name of a file to exclude or confirm the existence of child pornography within that file. Individuals will intentionally mislabel directory structures, folder names, and filenames to hide the presence of child pornography. In other cases, an individual may not attempt to hide the child pornography but utilize a unique naming convention or organizational methodology which may inadvertently hide the presence of child pornography. In order to perform a comprehensive forensic examination, a computer forensic examiner must conduct an all-inclusive examination of every bit (or binary digit) on the particular electronic storage device.

33. Moreover, hard drives and other pieces of electronic media have unallocated space which might contain deleted files, records, relevant e-mails, other communications, and search terms related to the possession, receipt, and distribution of child pornography. Thus, without

looking at the entirety of the electronic media for evidence related to child pornography, the investigator may not find evidence relevant to the criminal investigation.

SEARCH METHODOLOGY TO BE EMPLOYED

34. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer system(s) and computer hardware to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);

b. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. surveying various file directories and the individual files they contain;

e. opening files in order to determine their contents;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

USE OF BIOMETRIC FEATURES TO UNLOCK ELECTRONIC DEVICES

35. The warrant I am applying for would permit law enforcement to compel STEVEN LEE GLOVER to unlock a device subject to seizure pursuant to this warrant that is his possession or for which law enforcement otherwise has a reasonable basis to believe is used by him using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. I have probable cause to believe that one or more of the electronic devices in the SUBJECT PREMISES are likely to offer its user the ability to use biometric features to unlock the device(s). Your

affiant knows that many smart phones use fingerprint sensor technology and facial recognition to unlock the phone.

c. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

d. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other

manufacturers have different names but operate similarly to Trusted Face.

e. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

f. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

g. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

h. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock

the device through a biometric feature may exist for only a short time.

Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, and the device is in STEVEN LEE GLOVER's possession or law enforcement otherwise has a reasonable basis to believe is used by STEVEN LEE GLOVER, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of STEVEN LEE GLOVER, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of STEVEN LEE GLOVER, and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of STEVE LEE GLOVER, and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

CONCLUSION

36. Based on the foregoing I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

I state under the penalty of perjury that the foregoing is true and correct.

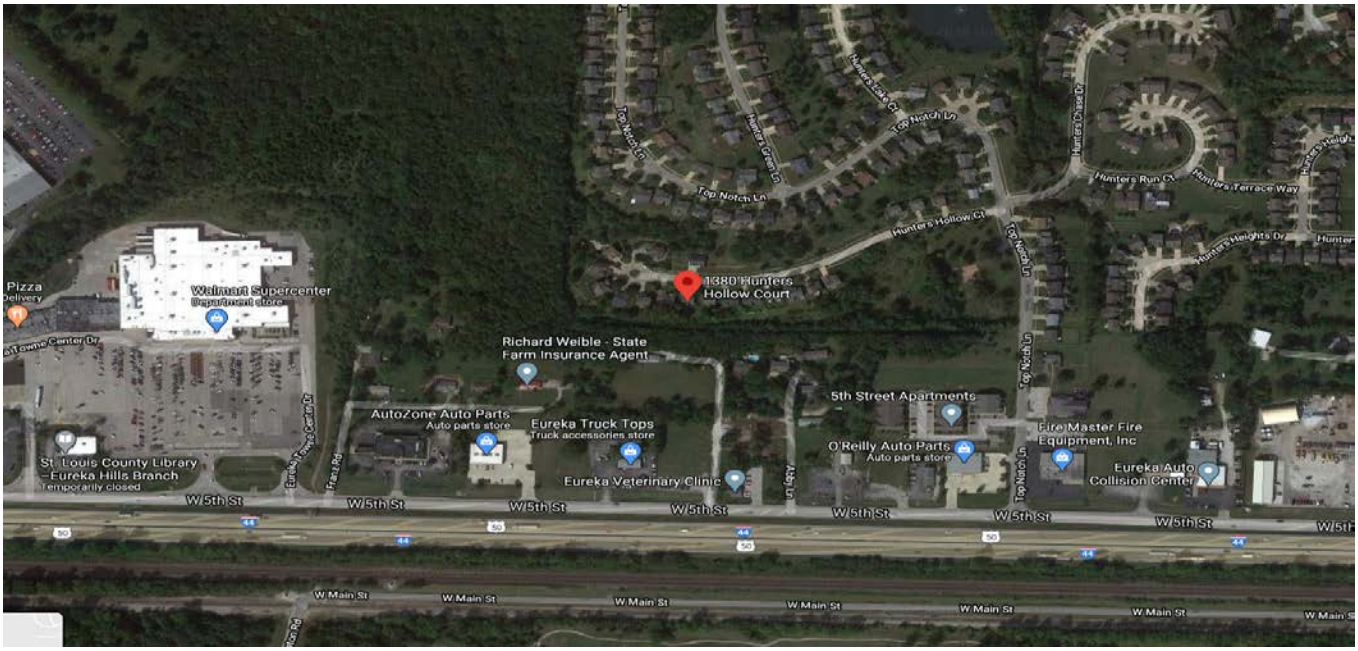
Gregory S. Marx
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 26th day of June, 2020.

NOELLE C. COLLINS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The premises known as 1380 HUNTERS HOLLOW CT., EUREKA, MISSOURI 63025, is referred to herein as the SUBJECT PREMISES and is described follows: a single family ranch with an attached two-car garage, as follows:



ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The following are to be seized from the SUBJECT PREMISES, as described in Attachment A: Evidence, instrumentalities and contraband concerning the violations of Title 18, United States Code, Sections 2251(a), 2252, and 2252A:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:

    a. Any computer, cell phone, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);

    b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and

    c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer and cell phone passwords and other data security devices designed to restrict access to or hide computer or cell phone software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, materials, emails, and/or internet history (in documentary or electronic form) pertaining to the possession, receipt, distribution, or production of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.

4. Any and all records, documents, records, materials, invoices, notes and/or materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Documents, records and/or materials regarding the ownership and/or possession of the SUBJECT PREMISES.

6. During the course of the search, photographs and/or videos of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.

7. During the execution of the search of the SUBJECT PREMISES, law enforcement personnel are also specifically authorized to obtain from STEVEN LEE GLOVER, if he is on the SUBJECT PREMISES at the time of execution of the warrant, the display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any electronic device, such as, but not limited to computers, computer hardware, cell phones, and tablets, requiring such biometric access subject to seizure pursuant to this warrant, that is, including pressing fingers or thumbs

against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the Device(s) found at the SUBJECT PREMISES that are in the possession of, or known to be used by, STEVEN LEE GLOVER,

(b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the electronic device(s)'s, which include, but are not limited to, computers, computer hardware, cell phones, and tablets, security features in order to search the contents as authorized by this warrant.

The terms "records," "documents," and "materials," as used in Attachment B, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).